IN THE CLAIMS:

Please amend claims 1-2, 4-10, 13, 22, 25, and 46, add claims 56-71, and cancel claims 3, 12, 26-43, and 48-55 as follows.

1. (Currently Amended) An apparatus, comprising:

~~a receiver configured to receive a message via a secure interface or directly from outside a telecommunications network;~~

a determiner configured to determine whether ~~the~~ a message received at a first network has been through a security check by determining whether or not the message has been received ~~via the secure interface~~ with security at a first layer;

a forwarder configured to forward the message within ~~the~~ said ~~telecommunications~~ first network regardless of the result of the determination; and

a modifier configured to modify the message so as to include a second layer indication ~~indicate~~ that the message has not been through a security check if the result of the determination is that the message has not been through a security check, wherein said second layer is a higher layer than said first layer.

2. (Currently Amended) ~~An~~ The apparatus according to claim 1, wherein the receiver is configured to receive ~~a~~ messages via a secure interface and a second network and directly from outside the ~~telecommunications~~ first network.

3. (Cancelled)

4. (Currently Amended) The ~~An~~ apparatus according to claim ~~3~~ 1, wherein the ~~receiver is configured to receive a~~ message ~~that~~ includes a second layer ~~an~~ identity header, and wherein the modifier is ~~further~~ configured to ~~add~~ include ~~the~~ said second layer indication ~~parameter to the~~ in said second layer identity header of the message.

5. (Currently Amended) The ~~An~~ apparatus according to claim 4, wherein the message comprises a session initiation protocol message.

6. (Currently Amended) The ~~An~~ apparatus according to claim 4, wherein the identity header comprises a P-Asserted-Identity.

7. (Currently Amended) The ~~An~~ apparatus according to claim 1, ~~further comprising:~~ wherein the message includes a second layer identity header, and wherein the modifier is further ~~a modifier~~ configured to modify the message so as to indicate that the message has not been through a security check by removing at least part of the second layer identity header~~, wherein the receiver is configured to receive a message that includes an identity header~~.

8. (Currently Amended) The ~~An~~ apparatus according to claim 7, further comprising:

a detector configured to detect whether the second layer identity header is of a particular type and if so to remove at least part of the header.

9. (Currently Amended) The ~~An~~ apparatus according to claim 7, wherein the message comprises a session initiation protocol message.

10. (Currently Amended) The ~~An~~ apparatus according to claim 8, wherein the detector is configured to detect whether the second layer identity header comprises a P-Asserted-Identity type.

11. (Cancelled)

12. (Cancelled)

13. (Currently Amended) The ~~An~~ apparatus according to claim 1, wherein the apparatus comprises an interrogating call session control function.

14. - 21. (Cancelled)

22. (Currently Amended) A system, comprising:

a security server; and

a network processing element, the security server being configured to receive a message ~~via a secure interface or directly from outside the system~~, determine whether the message has been through a security check by determining whether or not the message has been received ~~via the secure interface~~ with security at a first layer, if the result of the determination is that the message has not been through a security check modify the message so as to include a second layer ~~indicate~~ indication that the message has not been through a security check, wherein said second layer is a higher layer than said first layer, and forward the message to the network processing element regardless of the result of the determination.

23. (Currently Amended) The ~~A~~ system according to claim 22, wherein the security server is configured to ~~receive a~~ messages via a secure interface and another security domain and directly from outside the system.

24. (Currently Amended) The ~~A~~ system according to claim 22, wherein the network processing element is configured to,~~:~~

receive a message forwarded by the security server~~;~~, and

determine whether the message has been modified so as to include a second layer ~~indicate~~ indication that ~~it~~ the message has not been through a security check, and, if ~~it~~ the message has been so modified, perform one or more security checks in respect of the message.

25. (Currently Amended) A method, comprising:

~~receiving a message via a secure interface or directly from outside a telecommunications network;~~

determining that ~~the~~ a message received at a first network has not been through a security check by determining that ~~it~~ the message has not been received ~~via the secure interface~~ with security at a first layer;

modifying the message so as to include a second layer indication ~~indicate~~ that the message has not been through a security check, wherein the second layer is a higher layer than the first layer; and

forwarding the message within the ~~telecommunications~~ first network.

26.-45. (Cancelled)

46. (Currently Amended) An apparatus, comprising:

~~receiving means for receiving a message via a secure interface or directly from outside a telecommunications network;~~

determining means for determining whether ~~the~~ a message received at a first network has been through a security check by determining whether or not the message has been received ~~via the secure interface~~ with security at a first layer;

modifying means for, if the message is determined not to have been through a security check, modifying the message to include a second layer indication ~~indicate~~ that ~~it~~ the message has not been through a security check, wherein the second layer is a higher layer than the first layer; and

forwarding means for forwarding the message within the telecommunications network regardless of whether the message has been through a security check.

47.-55. (Cancelled)

56. (New) The method according to claim 25, wherein the message includes a second layer identity header, and comprising including said second layer indication in said second layer identity header of the message.

57. (New) The method according to claim 56, wherein the message comprises a session initiation protocol message.

58. (New) The method according to claim 56, wherein the identity header comprises a P-Asserted-Identity.

59. (New) The method according to claim 25, wherein the message includes a second layer identity header, and comprising modifying the message so as to include a second

layer indication that the message has not been through a security check by removing at least part of the second layer identity header.

60. (New) The method according to claim 25, further comprising: detecting whether the second layer identity header is of a particular type and if so removing at least part of the header.

61. (New) The method according to claim 60, wherein the message comprises a session initiation protocol message.

62. (New) The method according to claim 61, comprising detecting whether the second layer identity header comprises a P-Asserted-Identity type.

63. (New) The apparatus according to claim 1, wherein said security at a first layer is security applied to a message at a secure interface between two security domains.

64. (New) The apparatus according to claim 63, wherein said secure interface is a Za interface.

65. (New) The apparatus according to claim 1, wherein said forwarder is configured to forward said message over a Zb interface.

66. (New) The system according to claim 1, wherein said security at a first layer is security applied to a message at a secure interface between two security domains.

67. (New) The system according to claim 66, wherein said secure interface is a Za interface.

68. (New) The system according to claim 22, wherein said security server is configured to forward said message to said network processing element over a Zb interface.

69. (New) The method according to claim 25, wherein said security at a first layer is security applied to a message at a secure interface between two security domains.

70. (New) The method according to claim 69, wherein said secure interface is a Za interface.

71. (New) The method according to claim 25, comprising forwarding said message within said first network over a Zb interface.